DOCUMENT ID: SA26P011
VERSION: 1.0
DATE: 2026-07-06

CYBER SECURITY ADVISORY

Security Issues addressed in APROL R 4.4-01P5

CVE ID: CVE-2026-6900, CVE-2026-6901, CVE-2024-56337, CVE-2024-54677, CVE-2024-52317, CVE-2024-50379

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

Purpose

B&R has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, B&R immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If B&R is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of B&R's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

APROL < R 4.4-01P5

Vulnerability IDs

CVE-2026-6900, CVE-2026-6901, CVE-2024-56337, CVE-2024-54677, CVE-2024-52317, CVE-2024-50379

Summary

An update is available that resolves several vulnerabilities and updates 3rd party components in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could impact the availability of the product, spoof identities or elevate privileges.

Recommended immediate actions

The problem is corrected in the following product versions:

APROL >= R 4.4-01P5

B&R recommends that customers apply the update at earliest convenience.

The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual.

Vulnerability severity and details

Vulnerabilities have been identified in the product versions listed above. A remote attacker could exploit these vulnerabilities by sending specially crafted messages to the affected system node or by performing adversary-in-the-middle attacks. Successful exploitation may result in one or more of the following impacts:

- **Denial of Service** – the affected node becomes unresponsive or stops functioning
- **Identity Spoofing** – an attacker impersonates a legitimate user or system component
- **Information Disclosure** – confidential data is intercepted or exposed
- **Remote Code Execution** – arbitrary code is injected and executed on the affected node

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVE-2026-6900

An Improper Certificate Validation vulnerability in the LDAP Server Connector used in APROL version prior to R 4.4-01P5 may allow network-based attackers to conduct adversary -in-the-middle attacks causing information disclosure or identity spoofing.

CVSS

CVSS v3.1 Base Score: 7.4
CVSS v3.1 Temporal Score: 7.1
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/RL:O

CVSS v4.0 Score: 9.1
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CWE

CWE-295: Improper Certificate Validation

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-6900

CVE-2026-6901

An Untrusted Search Path vulnerability in the webserver used in APROL version prior to R 4.4-01P5 may allow authenticated local attackers to elevate their privileges.

CVSS

CVSS v3.1 Base Score: 7.7
CVSS v3.1 Temporal Score: 7.4
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/RL:O

CVSS v4.0 Score: 8.4
CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CWE

CWE-426: Untrusted Search Path

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-6901

CVE-2024-56337 (3rd Party vulnerability)

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache Tomcat. The previous mitigation for CVE-2024-50379 was incomplete, permitting an RCE on case insensitive file systems when the default servlet is enabled for write

CVSS

CVSS v3.1 Base Score: 9.8
CVSS v3.1 Temporal Score: N/A
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Score: N/A
CVSS v4.0 Vector: N/A

CWE

CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-56337

CVE-2024-54677 (3rd Party vulnerability)

Uncontrolled Resource Consumption vulnerability in the examples web application provided with Apache Tomcat leads to denial of service due to lacking data upload limits

CVSS

CVSS v3.1 Base Score: 5.3
CVSS v3.1 Temporal Score: N/A
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v4.0 Score: N/A
CVSS v4.0 Vector: N/A

CWE

CWE-400: Uncontrolled Resource Consumption

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-54677

CVE-2024-52317 (3rd Party vulnerability)

Incorrect object re-cycling and re-use vulnerability in Apache Tomcat. Incorrect recycling of the request and response used by HTTP/2 requests could lead to request and/or response mix-up between users

CVSS

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4.0 Score:	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-326: Inadequate Encryption Strength

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-52317

CVE-2024-50379 (3rd Party vulnerability)

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case-insensitive file systems when the default servlet is enabled for write (non-default configuration)

CVSS

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score:	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-50379

Workarounds

CVE-2026-6900

Enable TLS Certificate Verification System-Wide
Add the following configuration directive to the file /etc/openldap/ldap.conf:

TLS_REQCERT demand

This tells the LDAP client to require and verify the server's certificate.

Configure Certificate Verification for Each User Account
Each Linux user account (engineering, runtime, and operator accounts) needs its own configuration file that points to where its issuer certificates are stored.

Create a .ldaprc file in the home directory of each account and add the appropriate certificate directory path.

For Engineering Accounts: Create /home/<username>/.ldaprc and add:

TLS_CACERTDIR /home/<username>/ENGIN/cnf/GLOBAL_ENGINEERING/LDAP/issuers/

For Runtime and Operator Accounts: Create /home/<username>/.ldaprc and add:

TLS_CACERTDIR /home/<username>/RUNTIME/cnf/GLOBAL/LDAP/issuers/

Replace <username> with the actual Linux user account name.

Prepare the Certificate Directories
For each issuer certificate directory you created above, run this command to enable certificate verification:

openssl rehash <issuer certificate directory>

This command indexes the certificates so the system can find them quickly during verification.

Deploy Trusted Certificates
When you configure an external LDAP server, manually copy the server's trusted issuer certificate to the appropriate directories you created in “Configure Certificate Verification for Each User Account”.

CVE-2026-6901

Remove or replace all wildcard AliasMatch directives in the Apache configuration file /home/aprol-sys/APROL/cnf/apache2/apache2.conf with explicit aliases that refer to specific APROL system and project names.

For example, replace:

AliasMatch ^/(.*)/PROJECTS/(.*)/WEB/(.*)/DOCS/(.*) "/home/$1/ENGIN/PROJECTS/$2/WEB/$3/DOCS/$4"

with:

AliasMatch ^/<systemname>/PROJECTS/<projectname>/WEB/(.*)/DOCS/(.*) "/home/<systemname>/PROJECTS/<projectname>/WEB/$1/DOCS/$2"

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, B&R received information about this vulnerability through responsible disclosure

When this security advisory was issued, had B&R received any reports that this vulnerability was being exploited?

No, B&R had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

General security recommendations

For any installation of software-related B&R products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.

– Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
– When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following documents:

Defense in Depth for B&R products

Support

For additional instructions and support please contact your local B&R service organization. For contact information, see https://www.br-automation.com/en/about-us/locations/.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Version history

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date
1.0	all	Initial version	2026-07-06